TLP:WHITE

SICK PSIRT
Security Advisory

Eclipse Cyclone DDS Vulnerabilities have no impact on SICK picoScan150 & SICK picoScan120 products

Document ID:	SCA-2026-0004
Publication Date:	2026-02-13
CVE Identifiers:	CVE-2023-24011, CVE-2025-67109
Version:	1

Summary

Eclipse Cyclone DDS has known vulnerabilities and is used in SICK picoScan150 and SICK picoScan120 products starting with version 2.2.0. A current analysis confirms that the identified vulnerabilities (CVE-2025-67109 and CVE-2023-24011) do not affect SICK picoScan150 and SICK picoScan120. Both vulnerabilities relate exclusively to certificate-based security features of ROS 2 / DDS, which are not supported on SICK picoScan150 and SICK picoScan120 devices and cannot be enabled by customers. At this time, there is no indication of any potential risk to SICK picoScan150 and SICK picoScan120 related to these two vulnerabilities.

List of Products

Product	Part Number	Affected by
SICK picoScan120 with firmware >=2.2.0	1141751	CVE-2023-24011 Status: Known Not Affected Remediation: -
		CVE-2025-67109 Status: Known Not Affected Remediation: -
SICK picoScan150 with firmware >=2.2.0	1134607 1134608 1134609 1134610 1141395 1141396 1141397 1142269 1142270 1142272 1142273	CVE-2023-24011 Status: Known Not Affected Remediation: -
		CVE-2025-67109 Status: Known Not Affected Remediation: -

Vulnerability Overview

CVE-2023-24011 Exposure of Sensitive Information to an Unauthorized Actor

Summary: An attacker can arbitrarily craft malicious DDS Participants (or ROS 2 Nodes) with valid certificates to compromise and get full control of the attacked secure DDS databus system by exploiting vulnerable attributes in the configuration of PKCS#7 certificate's validation. This is caused by a non-compliant implementation of permission document verification used by some DDS vendors. Specifically, an improper use of the OpenSSL PKCS7_verify function used to validate S/MIME signatures.

CVE-2023-24011 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.2
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L
CWE identifier: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

CVE-2025-67109 Improper Validation of Certificate Expiration

Summary: Improper verification of the time certificate in Eclipse Cyclone DDS before v0.10.5 allows attackers to bypass certificate checks and execute commands with System privileges.

CVE-2025-67109 has been assigned to this vulnerability.
CVSSv3.1 base score: 10
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE identifier: CWE-298 (Improper Validation of Certificate Expiration)

General Security Practices

General Security Measures

As general security measures, SICK recommends to minimize network exposure of the devices, restrict network access and follow recommended security practices in order to run the devices in a protected IT environment.

Vulnerability Classification

SICK performs vulnerability classification by using the CVSS scoring system (*CVSS v3.1*). The environmental score is dependent on the customer's environment and can affect the overall CVSS score. SICK recommends that customers individually evaluate the environmental score to achieve final scoring.

Resources

SICK PSIRT Security Advisories:
https://www.sick.com/psirt

SICK Operating Guidelines:
https://www.sick.com/media/docs/9/19/719/special_information_sick_operating_guidelines_cybersecurity_by_sick_en_im0106719.pdf

ICS-CERT recommended practices on Industrial Security:
https://www.cisa.gov/resources-tools/resources/ics-recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

History

Version	Release Date	Comment
1	2026-02-13	Initial version